International Journal of Electrical, Computing Engineering and Communication (IJECC)

Vol. 1, Issue. 2, April – 2015 *ISSN (Online): 2394-8310*

Hidden Alertness Against Shoulder Surfing

S.Shobana[1], N.Belina[2], L.Rajamohan.AP[3]

[1]PG Student, Department of Computer Science Engineering, Sriram Engineering College, Chennai, INDIA

[2,3]Assistant Professor, Department of Computer Science Engineering, Sriram Engineering College, Chennai, INDIA

Abstract:- ***Security for an electronic device such as laptops, palmtops, smart phones, even locks in doors are either digitized by numbers or by patterns. Magnetic strip cards are common use for electronic payments and cash withdrawals. They can be easily used by swiping them through additional card readers. These passwords while used in public are unaware of human shoulder surfers who can easily identify the password. Cryptographic prevention techniques are hardly applicable because human users are limited in their capacity to process information. There have been alternative approaches considering asymmetry between user and system. In this paper, we propose a new method by which even using a recording device any surfer can't identify the password. A new technique is presented for secure personal identification number entry analyzing existing method under new framework. Effective PIN entry method is used to prevent the attackers by increasing the amount of short term memory required in attack. Methods proposed in this paper are 2-colored(BW), semi-4 colored(improved BW), pattern fixing(secret key).***

***Key Terms*: Human shoulder surfer, Personal Identification number, 2-colored, Semi 4-colored, Pattern fixing, Insidious advertence, Comprehensive grouping.**

I INTRODUCTION

Personal Identification Number is commonly used in various situations such as performing transactions in ATM, approval for transaction, unlocking the phone, locking individual app in phone. This PIN entry is being viewed by person nearby in public places. This kind of attack is threat to the use of PIN in public places for an emergency transaction. Pin hole cameras and skimmers are used as an external device for getting user information such as PIN number , card details. These device presence can't be identified by a common user.

To overcome this problem, a new method namely 2 color method(black and white) is used. This method has a disadvantage of using in a place with recording device such as cameras. This method has a disadvantage of using in a place with recording device such as cameras. Another secure PIN entry method used is semi-4 colored method wherein even a recording device cannot identify a single digit of PIN. Pattern matching method is used wherein colors are replaced by special symbols. This may be little time consuming but very secure than other methods.

Four criteria should be considered for the design of PIN entry method:

- ✓ Safety
- ✓ Functionality(Time to enter and fault entry)
- ✓ Consistent
- ✓ Charge Effectiveness(no extra hardware)

2 colored method is still considered secure against human opponent due to limited power of knowing .

Rationale 1: Opponent power of knowing and advanced skills are never considered.

Rationale 2: There does not exist formal procedure and quantity tool for analysis and comparison.

From the rationales mentioned, four contributions are made:

1. Develop a new method against the power of knowing called insidious advertence shoulder surfing to avoid attention and comprehensive grouping.
2. First use of static measurement of performance.
3. Considering 2 colored method as insecure.
4. Develop a defense technique.

Most of the shoulder surfing resistant PIN entry use the fact that the capacity of short term memory and real time processing performance of a human are very limited. User is provided with random challenges.

II PRELIMINARIES

A. Threat Model

User has to enter PIN value after which it is authenticated according to the registered PIN entry or otherwise rejected. This paper mainly focuses on weaker threat model. Surfer tries to observe the PIN value being entered but there is no recording device like camera. 2 colored method is considered secure in weaker threat model.

B. Security opinions for PIN entry methods

i. Guessing attack :

In Guessing attack, attacker guesses user PIN and inputs it to pass the test. They use the fact that distributions of PIN passwords are not uniform. Number of

attempts to guess the PIN value may be reduced and a random check is performed.

ii. Shoulder Surfing attack :

In shoulder surfing attack, attacker observes the PIN entry by looking over the user's shoulder and tries to find it. Opponent surfs multiple times with the user unaware of the attacks.

C. Related Work

Many research results have been presented. Yang Xiao (Yang Xiao, 2014) [13] proposed differentiated password scheme where the user has the freedom to choose virtual password ranging from weak to strong security. Viberpass (A.Bianchi I. , 2011)uses visual and haptic challenges. When the phone vibrates , user enters a false character through a standard keypad. If the phone remains quiet, user enters correct one. Yi-Lun (Yi-Lun Chen, 2013) (P.Dunphy, 2010) [14,5] proposed a simple text based graphical password. Justin Weaver and Kumar (Justin Weaver, 2011) (M.Kumar, 2007)[7,9] proposed Eye Dent system in which gaze points are automatically clustered to determine user's selected symbols.

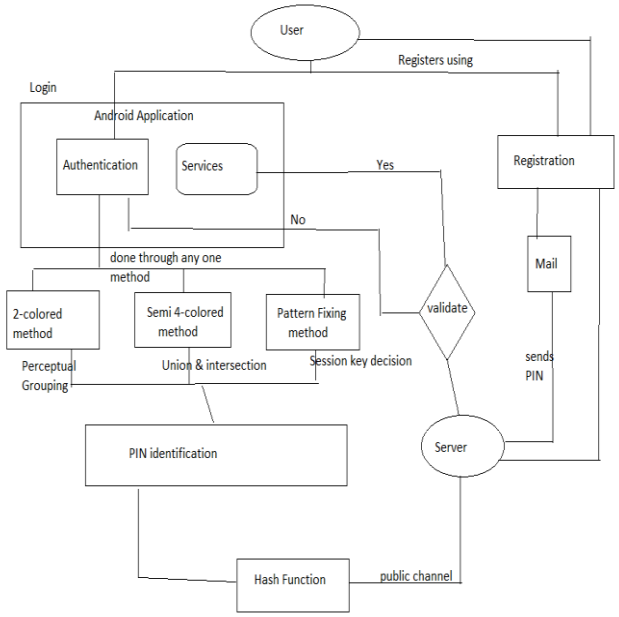
SSSL (T.Perkovic, 2009) [11] uses visual and audio challenges to enter PIN with reduced digit space. Bianchi (A.Bianchi I. K., 2012)[2] proposed uni -modal models in which passwords are encoded as sequence of vibration patterns without any visual information.

The design of PIN entry authentication system is based on multi-modal combinations of visual and non-visual content. Use of novel methods including audio cues, haptic cues and modulated visible light is proposed in counting clicks and beeps (A.Bianchi I. , 2011) (A.Bianchi I. K., 2012)[2,3]. Color PIN (A.D.Luca, 2010)[10] redefines a PIN such that PIN digit is a combination of number and a color. Phone lock (A.Bianchi I. , 2011)[3] and Time lock uses secondary channels.

Phone lock displays a graphical wheel with ten sectors. Time Lock uses PIN digit among 1..5. Switch PIN(A.D.Luca, 2010)[10], an effective PIN entry method is proposed by rendering a random mapping between switchable keypads. Passive adversaries are those that can passively monitor, intercept, analyze every part of the authentication procedure, except for the initial secret shared between the user and the system. To overcome this a new predicate based authentication service, PAS is introduced (X.Bai, Dec 2008)[1].

III PROPOSED SCHEME

A. Architecture Diagram



B. User Registration

User enters his basic details in an android application and once if he gets registered he is able to access his application in mobile phone. Once the user registration is completed, they will be provided with a unique PIN sent to their respective mail ID. Once it got validated user will be able to access application by entering username and password chosen at time of registration.

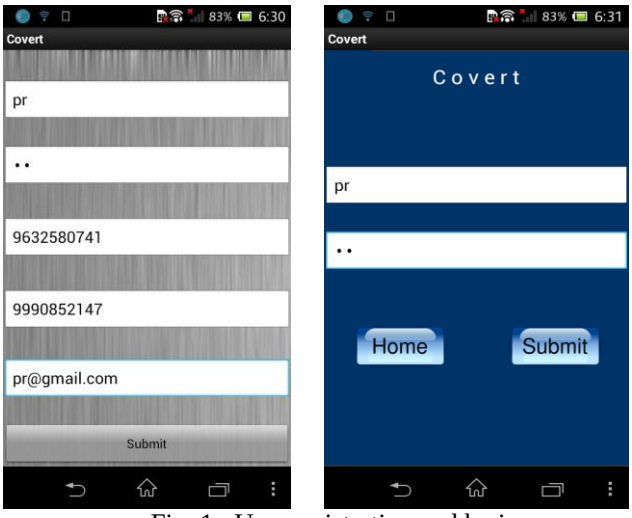


Fig .1 : User registration and login

C. 2-colored method (BW)

In this method regular keypad with digits 0 - 9 are equally split with 2 colors, half with black and half with white into two random halves. Each number is selected according to user key entry in each round. If the selected halves are memorized or written on paper and recalled to derive their grouping patterns, the shoulder surfer could identify a single digit of PIN. Even a recording device helps in identifying single PIN. In each round, regular numeric keypad is colored at random. User knows the correct PIN digit and can answer its color by pressing the separate key for black and white placed below. A common 4-digit PIN requires 4-5 iterations.

Demerits/Insecurity of 2 colored method:

- ✓ Static based analysis
- ✓ Reduce the number of visual things stored in short term memory
- ✓ Perform parallel motor operations
- ✓ Comprehensive grouping

D. Semi-4 colored method (Improved BW)

A set of 4 colors is {blue, black, white, yellow} used. A numeric keypad of ten digits is displayed with two split colors in each numeric key and separate keys for four colors placed below. A color is chosen at random which could be either upper or lower one from the numeric keypad and is entered through the separate color key. This procedure is repeated for m rounds such that all the digits of PIN is identified by union and intersection. This method has the main advantage that even a recording device couldn't find any of the digit. Exactly 4 iterations are only performed for each digit.

Algorithm: Semi-4 colored PIN Entry: pseudo code using union and intersection

$A,B \leftarrow \gamma(\pi(A))$ {*primary sets: A,B,C,D}
$C,D \leftarrow \gamma(\pi(A))$
$O, P \leftarrow (\emptyset, \emptyset)$ {*eliminated sets: O,P,Q,R}
$Q,R \leftarrow (\emptyset, \emptyset)$
for $i = 1, \cdots, m$ **do**
$a, b, c, d \leftarrow \rho(P)$
display ($A \cup P$ and $B \cup O$) and ($C \cup R$ and $D \cup Q$)
input choice ε a, b, c, d
if choice = a **then**
$Q,R \leftarrow \gamma(\pi(O \cup P \cup B))$
$O, P \leftarrow \gamma(\pi(O \cup P \cup B))$
$C,D \leftarrow \gamma(\pi(A))$
$A,B \leftarrow \gamma(\pi(A))$
else if choice = b **then**
$Q,R \leftarrow \gamma(\pi(O \cup P \cup A))$
$O, P \leftarrow \gamma(\pi(O \cup P \cup A))$
$C,D \leftarrow \gamma(\pi(B))$
$A,B \leftarrow \gamma(\pi(B))$
else if choice = c **then**
$O, P \leftarrow \gamma(\pi(Q \cup R \cup D))$
$Q,R \leftarrow \gamma(\pi(Q \cup R \cup D))$
$A,B \leftarrow \gamma(\pi(C))$
$C,D \leftarrow \gamma(\pi(C))$
else
$O, P \leftarrow \gamma(\pi(Q \cup R \cup C))$
$Q,R \leftarrow \gamma(\pi(Q \cup R \cup C))$
$A,B \leftarrow \gamma(\pi(D))$
$C,D \leftarrow \gamma(\pi(D))$
end if
end for {*for loop runs for m rounds}
return A {*a single digit is identified}

E. Pattern Fixing method

This method is basically different from above methods wherein instead of using color combinations, special symbols are used such as %,@,+,#. It consists of 4 rounds. The first round is decision of special symbol and remaining three are fixing the special symbol to the corresponding PIN values. The symbols are randomly arranged which is displayed to the user. The user selects a symbol at random to be the pattern for session. Once the symbol is selected, it can

be positioned to each corresponding digit of PIN by moving it up or down using the buttons 'up' and 'down'.

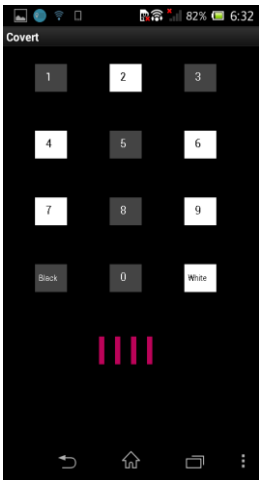


Fig.2(a). 2-colored

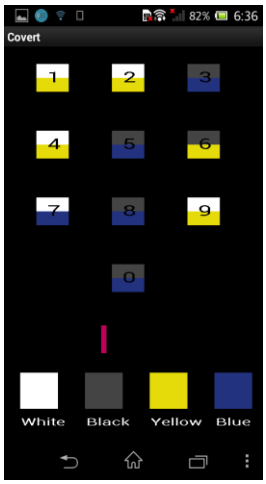


Fig.2(b) Semi-4 colored

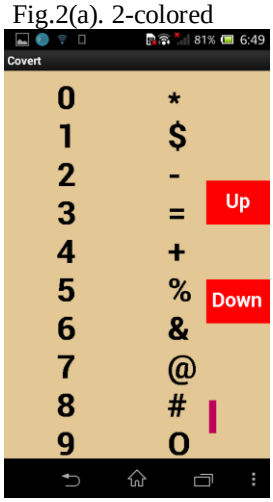


Fig.2(c) Pattern Fixing

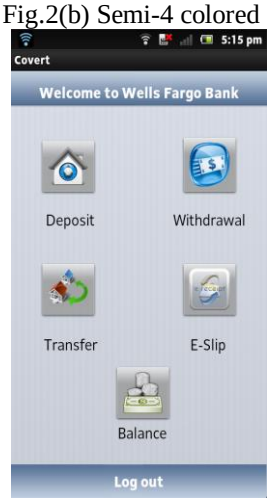


Fig.2(d)Services of ATM

F. Authentication and Services

Once the initial registration gets completed, the user gets a unique PIN number in his mail. The user can then enter the PIN number using any one of the methods mentioned above. Once entered, PIN is checked with the local database provided by Android OS using SQL Lite. A one way hash is generated for the validated PIN and is sent to server in public channel so that an active attacker cannot extract the PIN by monitoring the channel. Once got authenticated by server, the user can access to the services provided by mobile App. The services that are provided by mobile App are cash withdrawal, deposit and fund transfer. This can be done securely using the concept of virtual money.

IV RESULTS AND DISCUSSION

In this paper, a new security notion method is introduced and presented in theoretical and experimental technique to analyze security. The design for new security conviction method is devised using meaningful guidelines. Based on this guidelines, a PIN entry method is developed that has advanced security against human shoulder surfing attacks.

Even the proposed method is an effective counter measure against human shoulder surfing attacks, it cannot prevent recording attack. It is better to warn the users not to use this method in place with recording device. The weakness of 2-colored method in achieving both security and usability is truly challenging and prone to erroneous design due to lack of formal treatment.

Static based analysis of 2- colored method is compared with semi 4 colored method where four colors are shuffled at random in each iteration. PIN entry time of normal user varies for each method and is compared for n number of trails and participants.

V FUTURE WORK

The future work is to develop a new usably secure authentication method based on abundant evidence. Measures for preventing shoulder surfing attacks can in near future implemented in iPhone locks, door locks and even securing individual application of any android phones. Rather than Android OS, these methods are made to be implemented in any OS. Also, to quickly the hackers accessing the password, capturing their images through front camera is suggested.

REFERENCES

[1] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "PAS: Predicate-based authentication services against powerful passive adversaries," in *Proc. IEEE Annu. Comput. Security Appl. Conf.*, Dec. 2008, pp. 433–442.

[2] A. Bianchi, I. Oakley, and D.-S. Kwon, "*Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry*," Interact. Comput., vol. 24, no. 5, pp. 409–422, 2012.

[3] A. Bianchi, I. Oakley, V. Kostakos, and D.-S. Kwon, "*The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices*," in Proc. TEI, 2011, pp. 197–200.

[4] T. F. Brady, T. Konkle, and G. A. Alvarez, "A review of visual memory capacity: Beyond individual items and toward structured representations," *J. Vision*, vol. 11, no. 5, pp. 1–34, 2011

[5] P. Dunphy, A. P. Heiner, and N. Asokan, "A closer look at recognition based graphical passwords on mobile devices," in *Proc. ACM Symp. Usable Privacy Security*, 2010, pp. 1–12.

[6] W. S. Geisler and B. J. Super, "Perceptual organization of two dimensional patterns," Psychol. Rev., vol. 107, no. 4, pp. 677–708, 2000.

[7] Justin Weaver, Kenrick Mock, Bogdan Hoanca, "*Gaze-Based Password Authentication through Automatic Clustering of Gaze Points",* Computer Information Systems, University of Alaska,2011

[8] C. S. Kim and M.-K. Lee, "*Secure and user friendly PIN entry method*," in Proc. 28th Int. Conf. Consum. Electron., 2010, p. 5.1–1.

[9] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "*Reducing shoulder-surfing by using gaze-based password entry*," in Proc. SOUPS,2007, pp. 13–19

[10] A. D. Luca, K. Hertzschuch, and H. Hussmann, "*Color PIN: Securing PIN entry through indirect input*," in Proc. CHI, 2010, pp. 1103–1106.

[11] T. Perkovic, M. Cagalj, and N. Rakic, "*SSSL: Shoulder surfing safe login*," in Proc. Int. Conf. Softw., Telecommun. Comput. Netw., 2009, pp. 270–275.

[12] V. Roth, K. Richter, and R. Freidinger, "*A PIN-entry method resilient against shoulder surfing*," in Proc. CCS, 2004, pp. 236–245.

[13] Yang Xiao, Senior Member, IEEE, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky, "*Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password theft"*, IEEE systems journal, vol. 8, no. 2, JUNE 2014

[14] Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao, "*A Simple Text-Based Shoulder Surfing Resistant graphical Password Scheme",* IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan,2013